Uma Análise da Evolução e Características de Falhas em uma Rede de Telecomunicações de Médio Porte

Leandro A. de Sá Vieira e Ítalo Cunha

[1]Departamento de Ciência da Computação
Universidade Federal de Minas Gerais

{lvieira,cunha}@dcc.ufmg.br

Abstract. *The growth of the Internet and increasing demand for networked services require continued advances in communication technologies. Unfortunately, larger and more complex networks also suffer a higher number of incidents. Even though network incidents have significant negative impact on individuals and businesses, incident causes and characteristics are still poorly understood. In particular, network operators consider information about network incidents sensitive and private. In this work we analyze a dataset of network incidents on a regional Brazilian transit network with presence in five states. Our results further our understanding of transit network incidents, particularly as a function of network evolution. As an example, we find that the transition from circuit switching to packet switching technology led to an* increase *in the rate of incidents but also to a* decrease *in time to incident resolution.*

Resumo. *O crescimento da Internet e da demanda por serviços em rede dependem de avanço contínuo das tecnologias de comunicação. Porém, o crescimento da rede e de sua complexidade resultam em aumento do número de incidentes. Apesar do grande impacto de incidentes de rede no cotidiano de pessoas e empresas, nosso entendimento sobre suas causas e características ainda é muito limitado. Em particular, provedores consideram sensíveis e sigilosas informações sobre incidentes em suas redes e não divulgam estas informações. Neste trabalho analisamos um conjunto de dados contendo informações sobre incidentes na rede de uma operadora de telecomunicações de médio porte com atuação em cinco estados do Brasil. Nossos resultados melhoram nosso entendimento sobre incidentes de rede, especialmente em função da evolução da rede. Por exemplo, encontramos que a transição de sistemas de comutação por circuitos para sistemas de comutação por pacotes levou a um* aumento *da taxa de incidentes mas também a uma* redução *no tempo de resolução.*

1. Introdução

Conceber uma rede de telecomunicações imune a incidentes adversos é impossível. Diante disso, um melhor entendimento de incidentes—como frequência, características e causas—é essencial para instruir e aprimorar a gerência de redes [Govindan et al. 2016]. Melhor entendimento de incidentes permite a criação de novos procedimentos de verificação (do *software* e sua configuração, bem como do *hardware*)

[Gember-Jacobson et al. 2016, Beckett et al. 2016, Shaikh and Greenberg 2004], aprimoramento de rotinas para identificação das causas de incidentes [Dhamdhere et al. 2007, Nguyen et al. 2009, Kompella et al. 2005], implementação de ferramentas de monitoramento com maior cobertura e diagnóstico mais preciso [Mahimkar et al. 2008, Sommers et al. 2007, Cunha et al. 2009], ou desenvolvimento de mecanismos para contornar ou mitigar o impacto de incidentes [Peter et al. 2014, Katz-Bassett et al. 2012]. Infelizmente, muito poucos dados sobre incidentes de rede estão disponíveis publicamente, o que limita nossa capacidade de estudá-los. Isto acontece por que operadoras de telecomunicações consideram estas informações segredos de negócio sensíveis [Markopoulou et al. 2008, Dainotti et al. 2011, Turner et al. 2010].

Operadoras de telecomunicações investem esforço significativo para solucionar os inevitáveis incidentes de rede e garantir disponibilidade (*uptime*) da rede. Um relatório da Cisco indica que recursos humanos são 50% do custo de operação de uma rede [Cisco 2011]. Centros de gerência de rede empregam técnicos responsáveis por atividades como a conexão de novos clientes, expansão da infra-estrutura e configuração de dispositivos. Além disso, os centros de gerência também empregam plantão 24/7 para resposta a incidentes. Centros de gerência utilizam sistemas de rastreamento de incidentes (*issue tracking*) para coordenar a ação dos técnicos.

Neste trabalho caracterizamos dezenas de milhares de registros de incidentes no sistema de rastreamento do centro de gerência de uma operadora de telecomunicações com atuação em cinco estados no Brasil. Os registros cobrem incidentes que ocorreram entre janeiro de 2009 e setembro de 2016.

Nós avaliamos os registros de incidentes em quatro dimensões: tecnologia, causa do incidente, localização geográfica e ao longo do tempo. Quanto à tecnologia, contrastamos incidentes em dispositivos de comutação por circuitos (PDH/SDH) e incidentes em dispositivos de comutação de pacotes (Metro Ethernet e GPON-FTTH). Quanto à causa do incidente, consideramos causas como erros de configuração ou rompimento de fibra óptica. Quanto à localização geográfica, estudamos características de incidentes em capitais e no interior. E quanto ao tempo, o longo período de cobertura dos registros nos permite estudar características dos incidentes em função da evolução da rede. Caracterizamos os incidentes principalmente em função dos componentes do tempo de resolução (e.g., tempo de diagnóstico, tempo de análise e tempo para alocação de equipe de campo) e do tempo entre ocorrências de incidentes.

Nossos resultados melhoram nosso entendimento do impacto da evolução de uma rede sobre falhas e do impacto das falhas sobre o desempenho da rede. Por exemplo, encontramos que a frequência de incidentes em um enlace diminui à medida que seu tempo em produção aumenta; que a tecnologia de um enlace impacta a frequência de incidentes e a necessidade de intervenção em campo; que algumas causas de incidentes não são bem identificadas; e que enlaces no interior apresentam falhas com frequência maior que enlaces em capitais.

Nossos resultados podem direcionar esforços de operadores para tentar reduzir o tempo e custo de resolução de incidentes ou ajudar pesquisadores identificarem novos desafios de gerenciamento em redes modernas.

2. Estrutura da Rede

Infra-estrutura física. A rede analisada tem extensa infra-estrutura em um estado do Brasil, e mantém presença também em outros quatro estados vizinhos. A rede possui equipamentos em mais de 1000 localidades distintas. Interconexões entre PoPs do *backbone* são realizadas em topologia de anel, o que fornece certa redundância contra particionamento da rede. O *backbone* utiliza enlaces de comutação por circuito com taxas de transmissão a partir a 155 Mbps e enlaces de comutação por pacotes com taxas de transmissão a partir de 1 Gbps. A grande maioria dos enlaces entre PoPs utilizam fibra óptica e uma minoria utiliza radiofrequência. A infra-estrutura dos PoPs varia, mas geralmente inclui sistema de refrigeração, transformadores de corrente alternada em corrente contínua, sistema de energia sobressalente (baterias ou geradores a combustão), distribuidor óptico para organização do cabeamento e racks acomodando os equipamentos.

A rede tem capacidade agregada para aproximadamente 250 Gbps de tráfego externo, sendo 50 Gbps em três pontos de troca de tráfego (PTT) nacionais, 40 Gbps de trânsito internacional, e 160 Gbps em enlaces ponto-a-ponto comerciais. A quantidade e capacidade de equipamentos provisionados em um PoP são provisionados de acordo com a densidade de clientes atendidos e o volume de tráfego no PoP. Os clientes geralmente são conectados aos PoPs utilizando topologia estrela.

Gerenciamento da rede. O centro de gerência de redes (CGR) emprega 21 técnicos responsáveis por monitorar e realizar atividades corretivas 24/7. O CGR realiza monitoração pró-ativa na infra-estrutura dos PoPs através de sensores que reportam anomalias físicas, como aumento de temperatura e falta de energia. O monitoramento da rede possui um maior foco nos enlaces de *backbone*, onde incidentes têm impacto muito mais significativo. O monitoramento da rede é realizado através de ferramentas que detectam eventos como quedas de links, perda de pacotes e congestionamentos.

Um incidente pode ser detectado por processos de monitoramento ou informado através de contato realizado por um cliente. Após a notificação de um incidente, ele é tratado segundo o fluxograma na figura 1. Um técnico do centro de gerência analisa o incidente para tentar identificar o problema. Se um técnico não conseguir identificar o problema, outro técnico é atribuído para analisar o incidente. Após identificado o problema, um técnico decide se é necessário intervenção local via equipe de campo ou se o incidente pode ser solucionado remotamente.[1] Caso seja necessária intervenção local, uma equipe de campo é escalada e despachada. Após intervenção local, a falha é reavaliada pelo centro de gerência.

As equipes de campo são geograficamente distribuídas em localidades estratégicas, trabalhando em escalas de revezamento mantendo disponibilidade para acionamento 24/7. As capitais concentram cerca de 40% das equipes de campo. Geralmente cada equipe é formada por técnicos de equipamentos, responsáveis por atendimento nas instalações de clientes e PoPs, técnicos de fibra óptica, responsáveis pela manutenção na rede óptica, e técnicos de trabalho pesado, responsáveis por serviços como o lançamento de cabos entre postes.

[1]Comutadores e roteadores de propriedade da operadora instalados nos clientes podem ser acessados remotamente através de uma VLAN de gerência. Aproximadamente 90% dos equipamentos legados como modems PDH e conversores de mídia permitem gerencia remota.

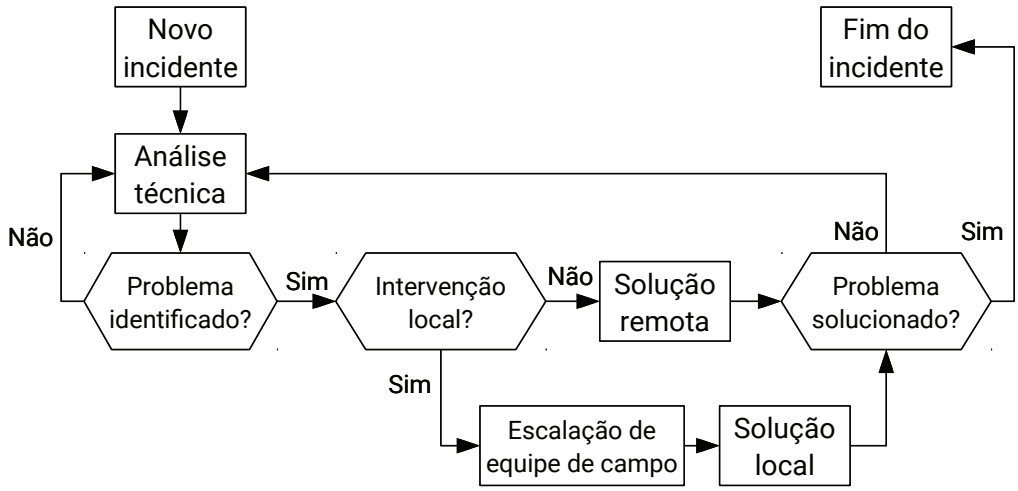


Figura 1. Fluxograma do tratamento de um incidente.

3. Conjunto de dados

Para cada incidente de rede identificado é aberto um registro num sistema de rastreamento de incidentes onde são inseridas informações sobre o tratamento do incidente até sua resolução. Nosso conjunto de dados contém dezenas de milhares de registros de falhas cobrindo sete anos de operação da rede, de janeiro de 2009 até setembro de 2016. A maioria (85%) dos registros foram originados a partir de reclamações realizadas pelos clientes e 15% foram originados de monitoramento pró-ativo da rede. Os dados são considerados sensíveis pela operadora e privados. Similar a outros trabalhos, acordamos com a operadora de focar nossos resultados em uma análise relativa dos incidentes de rede.

O primeiro técnico atribuído a um incidente é do centro de gerência e responsável pela análise inicial. A análise de um incidente pode levar à identificação do problema ou à atribuição do incidente a outro técnico que irá continuar a análise. Cada vez que um técnico é atribuído a um incidente, seu nome, equipe e horário de atribuição são registrados no sistema. Cada vez que um técnico termina sua análise, o horário do término também é registrado no sistema.

Como os registros são preenchidos manualmente, as informações inseridas podem conter erros ou imprecisões. Para reduzir o impacto de erros de preenchimento em nossa análise, agregamos períodos de tempo e desconsideramos o tempo de análise de cada técnico atribuído a um incidente. Definimos o *tempo de análise* de um incidente como o período entre os instantes de abertura do registro do incidente e de identificação do problema. Definimos o *tempo de solução* de um incidente como o período entre os instantes de abertura e de fechamento do registro. (Algumas vezes a equipe de campo acionada continua trabalhando *in loco* após o fechamento de um registro; não contabilizamos este período no tempo de solução do incidente.) Também filtramos registros de incidentes incompatíveis com o fluxograma mostrado na figura 1. Em particular, filtramos 3,5% de registros de incidentes nos quais a equipe solucionadora foi acionada antes da abertura do incidente. Filtramos também 38% dos incidentes cuja causa no sistema estava marcada como "não procedente": em sua maior parte incidentes reportados por clientes cuja causa

CAUSA	EXEMPLO DE DESCRIÇÃO
Configuração	"IP configurado erroneamente", "Cross conexão refeita"
Hardware	"Mau contato no cabo UTP", "Defeito na interface óptica"
Energia	"Falta de energia comercial", "Defeito na fonte de alimentação"
Rompimento	"Cabo óptico rompido", "Cabo óptico atenuado"
Outros	"Normalizou sem intervenção", "Falha na operadora parceira"

Tabela 1. Classificação de causas de incidentes.

não está na rede da operadora (e.g., incidentes na rede do próprio cliente).

Um registro de incidente contém ainda campos explícitos para identificação do dispositivo onde o incidente foi detectado, uma descrição da causa do incidente, localização geográfica e equipes envolvidas no solucionamento. Utilizamos estes registros para analisar os incidentes sob diferentes pontos de vista. Os registros possuem também um campo para descrição detalhada da causa e ações tomadas para solucionamento. Utilizamos este campo para melhor entender os incidentes.

4. Método de análise

Classificaçao dos incidentes. Nós classificamos os incidentes em quatro dimensões distintas. A primeira dimensão classifica incidentes por *tipo de tecnologia do enlace*, que pode ser de três tipos: enlaces de comutação por circuito PDH/SDH, utilizado em conexões entre PoPs e em serviços de *last mile* providos para outras operadoras; enlaces de comutação de pacotes Metro Ethernet, utilizado em conexão entre PoP e no acesso de clientes; e enlaces GPON-FTTP (*fiber to the premises*) que atende uma área residencial com internet, voz e TV a cabo.

A segunda dimensão classifica incidentes por *localização geográfica*: consideramos que incidentes podem ocorrer na capital ou no interior do estado onde a operadora concentra sua infra-estrutura. A terceira dimensão classifica incidentes por *tipo de causa*; classificamos os 251 identificadores de causa de incidente no sistema de rastreamento nas cinco classes mostradas na tabela 1. A tabela mostra alguns exemplos de identificadores de causa associados a cada classe. Por último, na quarta dimensão classificamos incidentes por *ano de ocorrência*.

Características dos incidentes. Caracterizamos três métricas principais dos incidentes: o tempo de solução (tempo de abertura e fechamento de um registro, seção 3), o tempo de reparo em campo e o tempo entre incidentes. Quando uma equipe solucionadora é acionada, um técnico analisa o incidente para escalar uma equipe de campo adequada. Nós descartamos esse tempo de análise; assim, o *tempo de reparo em campo* considera apenas as atividades realizadas exclusivamente por equipes de campo. O *tempo entre incidentes* é calculado por enlace, subtraindo o tempo de abertura de cada par de registros de incidentes concecutivos no mesmo enlace. Observamos que cerca de 3% dos pares de incidentes consecutivos ocorriam no mesmo dia e, na maioria dos casos que analisamos manualmente, eram casos de duplicidade no sistema. Em nossa análise consideramos apenas um registro de incidente por dia em cada enlace.

5. Resultados

Nesta seção apresentamos os resultados da análise dos registros de incidente. Mostramos uma visão geral da frequência e distribuição dos incidentes (seção 5.1) e analisamos os incidentes sob cada uma das dimensões definidas na seção 4 (seções 5.2–5.4).

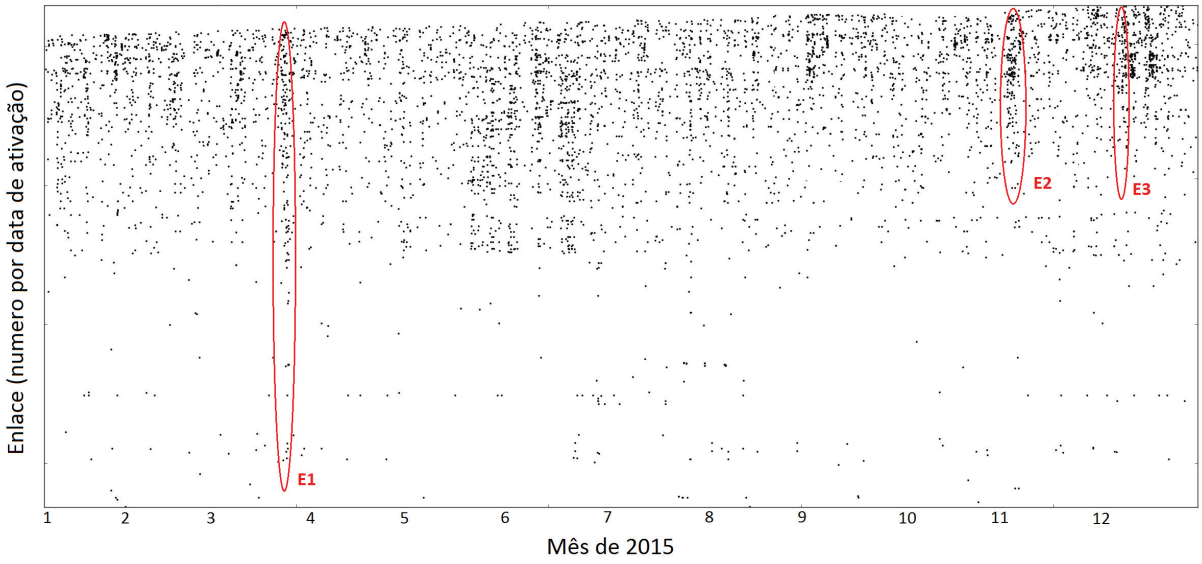


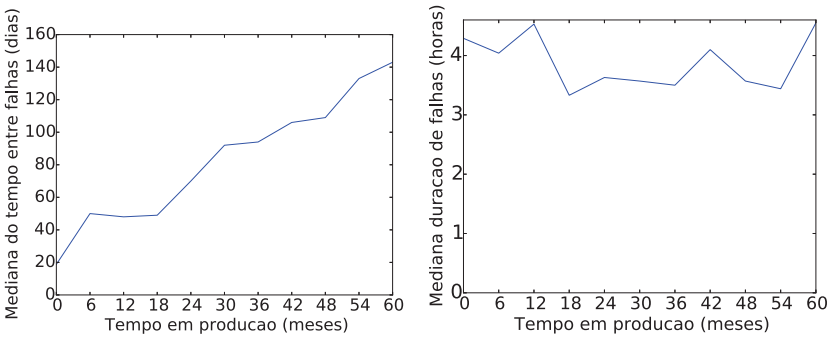
Figura 2. Visão geral dos incidentes de rede registrados em 2015. Os enlaces são ordenados ao longo do eixo Y pela data de ativação. Cada ponto representa o instante de abertura de um registro de incidente de rede.

5.1. Visão geral dos incidentes

A figura 2 mostra a visão geral dos incidentes de rede no ano de 2015. O eixo x mostra o tempo, o eixo y mostra os enlaces e cada ponto mostra o instante de abertura de um registro de incidente. Os enlaces estão ordenados ao longo do eixo y pela sua data de ativação (por isso o triangulo sem incidentes no canto superior esquerdo).

Mostramos os dados de 2015 pois em 2015 ocorreram 71% dos eventos que afetaram mais de 100 enlaces em nosso conjunto de dados. Resultados para outros anos são qualitativamente similares. Identificamos três dos eventos que afetaram mais de 100 enlaces em 2015 na figura 2 com círculos vermelhos.

O evento E1 resultou em incidentes em mais de 110 enlaces. O problema foi um duplo rompimento óptico que tirou de operação os enlaces principal e de redundância de um anel 10Gbps que conecta a capital com o interior do estado. No evento E2 temos representado um ciclo na rede de comutadores camada 2. Esse evento atingiu 151 enlaces de acesso de clientes, que ficaram inoperantes por duas horas, e foi causado por um erro de configuração. O evento E3 deixou 124 enlaces inoperantes por uma hora e meia e foi causado por outro ciclo na rede de comutadores camada 2 provocado por mal funcionamento dos comutadores de um anel 20Gbps. Para solucionar os incidentes foi necessário abrir um lado do anel e posteriormente atualizar o *firmware* de todos os comutadores envolvidos.



(a) Tempo entre incidentes (b) Tempo de resolução

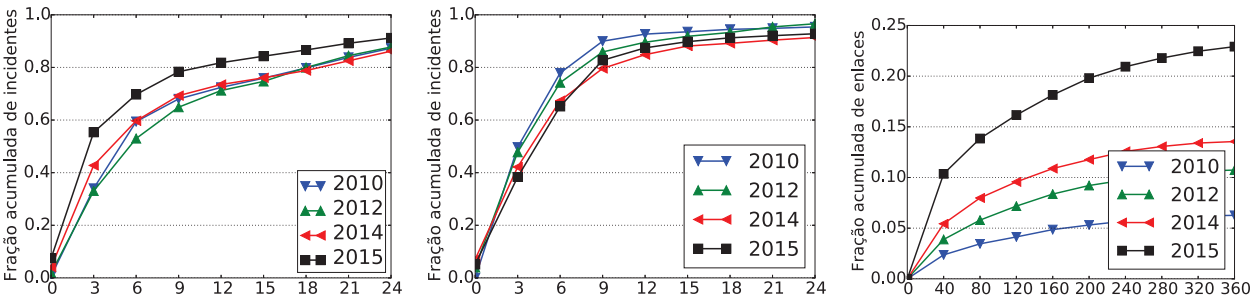
Figura 3. Características de incidentes em função do tempo que o enlace está em produção.

A figura 2 é similar a resultados anteriores caracterizando falhas em redes de trânsito [Markopoulou et al. 2008, Turner et al. 2010]. A figura mostra bandas verticais resultantes de incidentes ou atividades de manutenção que afetam vários enlaces. A figura mostra também (pequenas) bandas horizontais resultantes de enlaces com incidentes recorrentes.

A figura 2 mostra ainda que incidentes se concentram em enlaces ativados mais recentemente. A figura 3(a) confirma e quantifica essa observação mostrando a mediana do tempo entre falhas em função do tempo em produção (i.e., tempo desde a ativação de um enlace). A figura 3(b) mostra a mediana do tempo de resolução de incidentes em função do tempo em produção. Apesar dos enlaces em produção a menos tempo apresentarem maior frequência de incidentes, vemos que o tempo de resolução é pouco afetado pelo tempo em produção.

5.2. Evolução de incidentes ao longo do tempo

A figura 4(a) mostra o tempo de solução de falhas por ano. O tempo médio de solução de incidentes permaneceu estável entre 2009 e 2014, com tempo de solução médio mínimo de 9,3 horas (em 2010) e máximo de 10,0 horas (em 2013). Porém, percebemos uma significativa redução em 2015, com tempo médio de solução de 6,8 horas. Esta redução deve-se a um aumento significativo da fração de falhas que ocorrem em enlaces do tipo Metro Ethernet. Como mostraremos na seção 5.3, enlaces Metro Ethernet possuem tempo



(a) Tempo de solução (h) (b) Tempo de trabalho em campo (h) (c) Tempo entre incidentes (dias)

Figura 4. Análise de incidentes por ano.

Tabela 2. Evolução do perfil da infra-estrutura. Dados mostrados em escala relativa para para manter em sigilo os valores absolutos.

Ano	PDH/SDH		Metro Ethernet		GPON	
	Enlaces	Incidentes	Enlaces	Incidentes	Enlaces	Incidentes
2009	96,6%	94,2%	3,4%	5,8%	0,0%	0,0%
2010	92,3%	88,4%	4,6%	7,6%	3,0%	3,9%
2011	89,4%	75,5%	5,8%	19,7%	4,7%	4,8%
2012	85,7%	51,3%	6,7%	41,3%	7,5%	7,3%
2013	81,6%	48,7%	9,3%	40,7%	9,0%	10,6%
2014	76,5%	33,2%	15,2%	57,5%	8,2%	9,2%
2015	72,9%	22,0%	18,3%	68,8%	8,8%	9,2%
2016	68,7%	14,8%	22,5%	77,0%	8,8%	8,1%

de solução de incidente menor que as outras tecnologias empregadas pela operadora.

Apesar da aparente melhora no tempo de solução de incidentes em 2015, a figura 4(b) mostra que o tempo de trabalho em campo não apresenta melhora ao longo dos anos. Pelo contrário, vemos um pequeno aumento do tempo de trabalho em campo, o que pode ser resultado de expansão geográfica da rede ao longo dos anos e do aumento do número de clientes, o que exige mais deslocamentos das equipes de campo.[2]

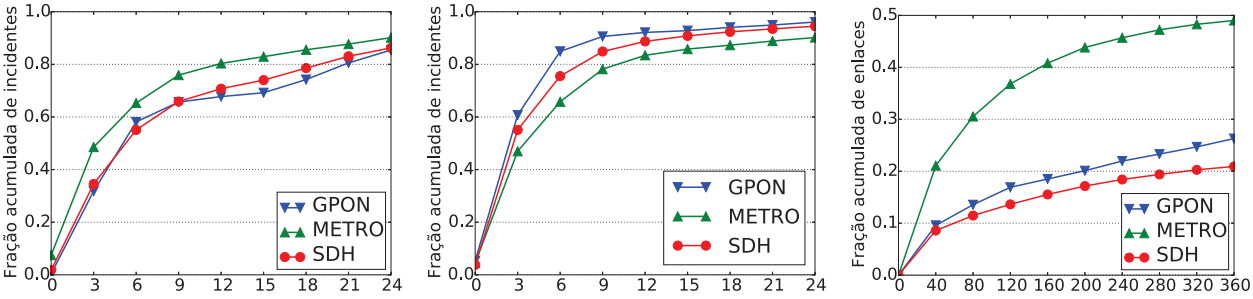
As longas caudas das distribuições nas figuras 4(a) e (b) devem-se geralmente a interrupções no trabalho de solução do incidente devido a fatores externos como a falta de segurança para o trabalho da equipe de campo, falta de autorização para atividade de manutenção em instalações de clientes, ou espera por equipamento.

A figura 4(c) mostra a distribuição do tempo entre incidentes nos enlaces. Calculamos o período entre pares de incidentes consecutivos em cada enlace. Contabilizamos cada par no ano de ocorrência do segundo incidente no par (o mais recente). Cortamos o eixo y em 0,25 para melhorar a legibilidade. As distribuições não chegam a 1,0 por que uma fração significativa dos enlaces não sofrem nenhum incidente; contabilizamos estes enlaces no gráfico com um tempo entre incidentes infinito. Percebemos uma clara redução do tempo entre incidentes, um resultado negativo. Novamente, este resultado deve-se ao aumento da fração de enlaces Metro Ethernet, que possui maior taxa de incidentes (seção 5.3).

5.3. Características de incidentes por tipo de tecnologia de enlace

O perfil da infra-estrutura de rede da operadora mudou ao longo dos anos em função de avanços tecnológicos e aumento do número de clientes. A tabela 2 mostra a fração de enlaces da rede de cada tipo das três tecnologias utilizadas. Observamos uma substituição gradativa dos enlaces PDH/SDH por enlaces Metro Ethernet, e o crescimento de enlaces GPON. A tabela 2 também mostra a fração de incidentes para cada tipo de tecnologia. Vemos que os enlaces Metro Ethernet apresentam incidentes muito mais frequentemente do que enlaces PDH/SDH e GPON.

[2]Os registros de incidente não contabilizam o tempo de deslocamento. Alternativamente, tentamos quantificar o deslocamento da equipe de campo (e.g., via consumo de combustível) para embasar essa hipótese mas não conseguimos obter esta informação.



(a) Tempo de solução (h) (b) Tempo de trabalho em campo (h) (c) Tempo entre incidentes (dias)

Figura 5. Análise de incidentes por tecnologia.

A figura 5 é análoga à figura 4, porém particiona os incidentes por tecnologia do enlace em vez de por ano de ocorrência. A figura 5(a) mostra que enlaces Metro Ethernet têm os menores tempos de solução de incidentes. Este resultado deve-se ao fato que incidentes em enlaces Metro Ethernet são resolvidos remotamente, sem intervenção via equipe de campo, 44% das vezes; incidentes em enlaces PDH/SDH e GPON podem ser resolvidos remotamente apenas 9% e 11% das vezes, respectivamente.

A figura 5(b) mostra a distribuição do tempo de trabalho das equipes de campo. Enlaces GPON têm menor tempo de trabalho em campo, provavelmente por que estes enlaces se concentram em regiões específicas onde existem planos de alta velocidade usando vibra óptica, o que reduz o tempo de deslocamento e heterogeneidade dos dispositivos. Apesar da menor necessidade de intervenção em campo, incidentes em enlaces Metro Ethernet em geral possuem maior tempo de resolução em campo. Um fator é que as intervenções em campo podem ser feitas em instalações de clientes, sobre as quais a operadora não tem controle.

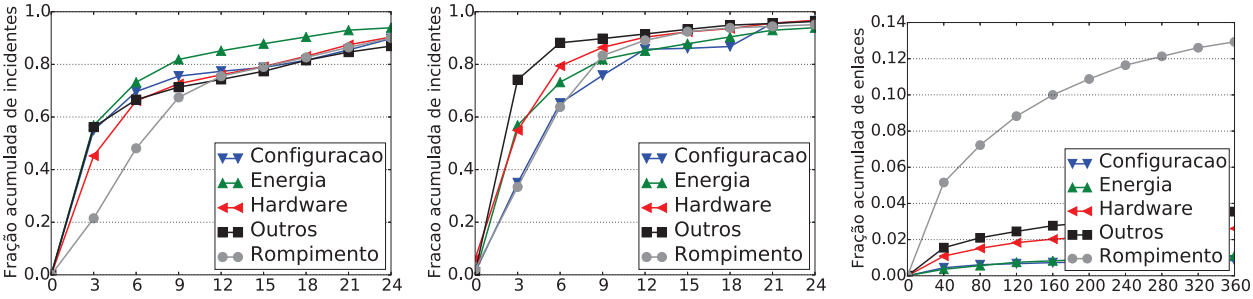
Por último, a figura 5(c) mostra a distribuição do tempo entre incidentes por enlace para cada uma das tecnologias de enlace. Note que o eixo y vai apenas até 0,5. A figura 5(c) confirma os resultados na tabela 2, confirmando que enlaces Metro Ethernet apresentam tempo entre falhas significativamente menor que enlaces PDH/SDH e GPON.

5.4. Características de incidentes por causa

A tabela 3 mostra a proporção de cada causa de incidente entre as tecnologias utilizadas. Vemos que a proporção de causas de incidentes é relativamente parecida entre todas as tecnologias utilizadas. Chamamos atenção para uma maior concentração de incidentes de configuração em enlaces Metro Ethernet e maior concentração de incidentes de *hardware* em enlaces GPON.

Tabela 3. Quantidade de incidentes por causa e tecnologia. Probabilidade de intervenção em campo em função da causa do incidente.

	PDH/SDH	Metro Ethernet	GPON	Intervenção em campo
Hardware	24.9%	22.4%	39.1%	80.6%
Configuração	4.0%	7.5%	5.3%	65.3%
Energia	7.7%	5.5%	1.1%	46.3%
Rompimento	47.0%	52.0%	52.6%	100.0%
Outros	16.3%	12.3%	3.1%	37.4%



(a) Tempo de solução (h) (b) Tempo de trabalho em campo (h) (c) Tempo entre incidentes (dias)

Figura 6. Análise de incidentes por causa de falhas.

A figura 6(a) mostra que os incidentes de rompimento possuem os maiores tempos de solução. Isto é esperado, visto a necessidade de intervenção de equipe de campo e necessidade de realizar fusões de fibra óptica. Incidentes de energia e configuração em geral apresentam menor tempo de resolução e as menores taxas de intervenção em campo.

Porém, como mostrado na figura 6(b), quando há necessidade de envio de equipe de campo na solução de incidentes de configuração, o tempo de trabalho em campo é semelhante ao de incidentes de rompimento. Este resultado ilustra a complexidade da configuração de redes modernas e a necessidade de modernos mecanismos de verificação e auxílio à gerência.

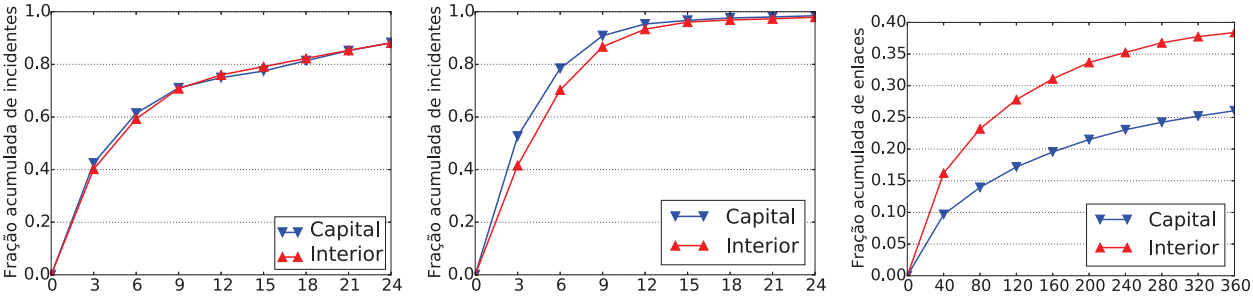
A figura 6(c) mostra o tempo entre incidentes com a mesma causa em todos os enlaces na rede da operadora. Enlaces sem incidentes ou com apenas um incidente de uma causa são contabilizados com tempo entre incidentes infinito. A figura mostra que, em geral, enlaces apresentam incidentes com a mesma causa com frequência muito baixa. (Note que o eixo y vai até 0,14.) A exceção são incidentes de rompimento, que é a causa mais comum (tabela 3) e reincidente.

5.5. Características de incidentes localização geográfica

A localização de um enlace, i.e., capital ou interior, é determinada de acordo com a localização da ponta mais distante da capital. Se um enlace interliga um concentrador em uma capital a um roteador de acesso de usuário no interior, consideramos que o enlace está no interior. De forma similar, se um enlace do *backbone* liga um PoP na capital a um PoP no interior, consideramos que o enlace está no interior. Utilizando esta classificação, 39% dos enlaces estão localizados no interior e totalizam 38% das falhas.

A figura 7(a) mostra que incidentes na capital e no interior têm tempos de solução similares. A figura 7(b) mostra que o tempo de recuperação em campo é menor para incidentes em capitais do que no interior. Este resultado é esperado, pois o tempo de recuperação em campo para enlaces inclui o tempo de deslocamento das equipes de campo. Como a rede do interior é mais espaçada geograficamente, o tempo de deslocamento de uma equipe técnica até o local do incidente é maior comparado ao tempo de deslocamento na capital. Consideramos a diferença de aproximadamente uma hora pequena, o que pode ser explicado pela boa distribuição geográfica das equipes de campo.

A figura 7(c) mostra que o tempo entre incidentes no interior é significativamente menor que nas capitais. (Note que o eixo y vai apenas até 0,4.) Este resultado pode ser



(a) Tempo de solução (h) (b) Tempo de trabalho em campo (h) (c) Tempo entre incidentes (dias)

Figura 7. Análise de incidentes por localização geográfica.

devido à diferença de infra-estrutura entre PoPs nas capitais e no interior. Apenas 39% dos enlaces estão no interior, espalhados em um número maior de PoPs. Outra explicação para a maior frequência de incidentes em enlaces no interior é que enlaces no interior ficam em produção por um período de tempo 31% menor que enlaces nas capitais (recorde que enlaces em produção por menor tempo apresentam maior frequência de falhas, figura 3(a)). Os equipamentos de acesso (como modems e switches) instalados pela operadora nos clientes são os mesmos, independentes da localização do cliente. Assim não consideramos que equipamentos são uma justificativa para as diferenças observadas.

6. Implicações práticas

Os resultados do presente trabalho podem ser aplicados para direcionar esforços na melhoria da operação de redes de telecomunicações, particularmente redes IP utilizando diferentes tecnologias de transmissão na camada de enlace.

Por exemplo, os resultados indicam que incidentes devidos a rompimento de fibra óptica possuem os maiores tempos de resolução. Esta informação pode motivar o desenvolvimento de novos procedimentos para resposta a este tipo de incidentes ou guiar o processo de expandão da rede para minimizar o impacto deste tipo de incidentes. De forma complementar, os resultados indicam que falhas em enlaces Metro Ethernet são as mais comuns. Este resultado motiva o desenvolvimento de ferramentas e processas que reduzam a frequência de incidentes nesses enlaces. Por último, os resultados podem ser utilizados para guiar o aprimoramento de sistemas de monitoramento, permitindo diagnóstico mais rápido e preciso de incidentes de rede.

7. Trabalhos relacionados

Caracterização de incidentes em redes. Outros trabalhos na literatura já caracterizaram incidentes em redes de trânsito. Apesar do objetivo comum de melhorar nosso entendimento sobre incidentes de rede, cada trabalho utiliza uma abordagem diferente, que depende dos dados disponíveis para estudo (que variam significativamente de uma rede para outra). Por exemplo, [Ghobadi and Mahajan 2016] utilizaram medições de qualidade de sinal para caracterizar falhas em enlaces ópticos enquanto [Govindan et al. 2016] utilizaram relatórios *post-mortem* de incidentes para entender suas causas e a importância de mecanismos que garantam disponibilidade da rede. Mais similar ao nosso trabalho são estudos de caracterização de registros de in-

cidentes [Markopoulou et al. 2008, Dainotti et al. 2011, Turner et al. 2010]. Alguns destes trabalhos utilizaram informações (*logs*) dos dispositivos da rede para corroborar as informações nos registros de incidentes; neste trabalho não tivemos acesso a *logs* dos dispositivos.

Monitoramento. Como informações sobre características de uma rede são essenciais para a operação da rede, execução de aplicações críticas e desenvolvimento de novas tecnologias, existe um grande esforço de pesquisa em ferramentas de monitoramento de rede. Os desafios estão em obter informações precisas a baixo custo (banda e processamaento) em um ambiente distribuído de larga escala, heterogêneo e repleto de fatores que interferem no monitoramento. Como exemplo, pesquisadores estudam soluções para detecção e localização de falhas [Katz-Bassett et al. 2012, Dhamdhere et al. 2007], congestionamento [Cardwell et al. 2016, Sommers et al. 2006], erros de configuração [Beckett et al. 2016, Gember-Jacobson et al. 2016], perda de pacotes [Sommers et al. 2007], *bufferbloat* [Gettys and Nichols 2011], dentre outros.

Ferramentas de monitoramento com e sem colaboração da rede. Ferramentas de monitoramento podem depender de colaboração por parte da rede monitorada, como acesso a informações coletadas por roteadores (e.g., [Mahimkar et al. 2009, Mahimkar et al. 2008, Shaikh and Greenberg 2004, Kompella et al. 2005]). Em geral, estas soluções obtém resultados mais precisos a menor custo, visto a melhor qualidade das informações. Estas ferramentas, porém, estão restritas aos operadores da própria rede. Os registros de incidentes caraterizados neste trabalho foram obtidos via uma parceria com a operadora de telecomunicações. Ferramentas de monitoramento que não dependem de colaboração por parte da rede monitorada coletam informações a partir de dispositivos externos (e.g., [Katz-Bassett et al. 2008, Kreibich et al. 2010, Chandrasekaran et al. 2015, Dischinger et al. 2010, Nikravesh et al. 2014, Quan et al. 2013]). Estas ferramentas trabalham com dados de menor visibilidade e são mais suscetíveis a interferências.

8. Conclusão

O crescimento da Internet e da demanda por serviços em rede dependem de avanço contínuo das tecnologias de comunicação e das soluções de monitoramento e gerência, essenciais para o rastreamento e solucionamento dos inevitáveis incidentes de rede. Neste trabalho caracterizamos um conjunto de registros de incidentes de uma na rede de uma operadora de telecomunicações de médio porte. Analisamos três características principais dos incidentes (tempo de solução, tempo de trabalho em campo e tempo entre incidentes) em quatro dimensões (tempo, tecnologia, causa e localidade geográfica).

Nossos resultados mostram que a frequência de incidentes em um enlace diminui à medida que permanece em produção. Nossos resultados mostram também que mudanças na frequência e no tempo de solução de incidentes são explicadas pela mudança no perfil das tecnologias utilizadas na rede: diferentes tecnologias apresentam frequência e tempo de solução de incidentes significativamente diferentes. Identificamos ainda possíveis pontos de melhora no processo de tratamento de incidentes, por exemplo, na identificação da causa de um incidente.

Nossos resultados apontam o impacto de cada dimensão nas características de incidentes, evidenciando problemas e possibilidades de melhoria. Nossos resultados podem ajudar operadores e pesquisadores a desenvolverem novas técnicas e processos para

tratamento de incidentes de rede.

Como trabalho futuro planejamos extender a nosso estudo para incluir *logs* coletados por comutadores e roteadores, complemetando os dados de registros e provendo melhor entendimento das causas e impactos de falhas.

Referências

Beckett, R., Mahajan, R., Millstein, T., Padhye, J., and Walker, D. (2016). Don'T Mind the Gap: Bridging Network-wide Objectives and Device-level Configurations. In *Proc. ACM SIGCOMM*.

Cardwell, N., Cheng, Y., Gunn, C. S., Yeganeh, S. H., and Jacobson, V. (2016). BBR: Congestion-Based Congestion Control. *ACM Queue*, 14(5).

Chandrasekaran, B., Smaragdakis, G., Berger, A., Luckie, M., and Ng, K.-C. (2015). A Server-to-server View of the Internet. In *Proc. ACM CoNEXT*.

Cisco (2011). The Economics of Networking. In *Technical Report*.

Cunha, I., Teixeira, R., Feamster, N., and Diot, C. (2009). Measurement Methods for Fast and Accurate Blackhole Identification with Binary Tomography. In *Proc. ACM IMC*.

Dainotti, A., Squarcella, C., Aben, E., Claffy, K. C., Chiesa, M., Russo, M., and Pescapé, A. (2011). Analysis of Country-wide Internet Outages Caused by Censorship. In *Proc. ACM IMC*.

Dhamdhere, A., Teixeira, R., Drovolis, C., and Diot, C. (2007). NetDiagnoser: Troubleshooting Network Unreachabilities Using End-to-end Probes and Routing Data. In *Proc. ACM CoNEXT*.

Dischinger, M., Marcon, M., Guha, S., Gummadi, K. P., Mahajan, R., and Saroiu, S. (2010). Glasnost: Enabling End Users to Detect Traffic Differentiation. In *Proc. USENIX NSDI*.

Gember-Jacobson, A., Viswanathan, R., Akella, A., and Mahajan, R. (2016). Fast Control Plane Analysis Using an Abstract Representation. In *Proc. ACM SIGCOMM*.

Gettys, J. and Nichols, K. (2011). Bufferbloat: Dark Buffers in the Internet. *Queue*, 9(11).

Ghobadi, M. and Mahajan, R. (2016). Optical Layer Failures in a Large Backbone. In *Proc. ACM IMC*.

Govindan, R., Minei, I., Kallahalla, M., Koley, B., and Vahdat, A. (2016). Evolve or Die: High-Availability Design Principles Drawn from Googles Network Infrastructure. In *Proc. ACM SIGCOMM*.

Katz-Bassett, E., Madhyastha, H., John, J. P., Krishnamurthy, A., Wetherall, D., and Anderson, T. (2008). Studying Black Holes in the Internet with Hubble. In *Proc. USENIX NSDI*.

Katz-Bassett, E., Scott, C., Choffnes, D. R., Cunha, I., Valancius, V., Feamster, N., Madhyastha, H. V., Anderson, T., and Krishnamurthy, A. (2012). LIFEGUARD: Practical Repair of Persistent Route Failures. In *Proc. ACM SIGCOMM*.

Kompella, R. R., Yates, J., Greenberg, A., and Snoeren, A. C. (2005). IP Fault Localization via Risk Modeling. In *Proc. USENIX NSDI*.

Kreibich, C., Weaver, N., Nechaev, B., and Paxson, V. (2010). Netalyzr: Illuminating The Edge Network. In *Proc. ACM IMC*.

Mahimkar, A., Yates, J., Zhang, Y., Shaikh, A., Wang, J., Ge, Z., and Ee, C. (2008). Troubleshooting Chronic Conditions in Large IP Networks. In *Proc. ACM CoNEXT*.

Mahimkar, A. A., Ge, Z., Shaikh, A., Wang, J., Yates, J., Zhang, Y., and Zhao, Q. (2009). Towards Automated Performance Diagnosis in a Large IPTV Network. In *Proc. ACM SIGCOMM*.

Markopoulou, A., Iannaccone, G., Bhattacharyya, S., Chuah, C. N., Ganjali, Y., and Diot, C. (2008). Characterization of Failures in an Operational IP Backbone Network. *IEEE/ACM Trans. Netw.*, 16(4):749–762.

Nguyen, H., Teixeira, R., Thiran, P., and Diot, C. (2009). Minimizing Probing Cost for Detecting Interface Failures: Algorithms and Scalability Analysis. In *Proc. IEEE INFOCOM*.

Nikravesh, A., Choffnes, D. R., Katz-Bassett, E., Mao, Z. M., and Welsh, M. (2014). Mobile Network Performance from User Devices: A Longitudinal, Multidimensional Analysis. In *Passive and Active Measurement Conference*.

Peter, S., Javed, U., Zhang, Q., Woos, D., Krishnamurthy, A., and Anderson, T. (2014). One Tunnel is (Often) Enough. In *Proc. ACM SIGCOMM*.

Quan, L., Heidemann, J., and Pradkin, Y. (2013). Trinocular: Understanding Internet Reliability Through Adaptive Probing. In *Proc. ACM SIGCOMM*.

Shaikh, A. and Greenberg, A. (2004). OSPF Monitoring: Architecture, Design and Deployment Experience. In *Proc. USENIX NSDI*.

Sommers, J., Barford, P., Duffield, N., and Ron, A. (2007). Accurate and Efficient SLA Compliance Monitoring. In *Proc. ACM SIGCOMM*.

Sommers, J., Barford, P., and Willinger, W. (2006). A Proposed Framework for Calibration of Available Bandwidth Estimation Tools. In *Proc. IEEE Symp. on Comp. and Comm.*

Turner, D., Levchenko, K., Snoeren, A., and Savage, S. (2010). California Fault Lines: Understanding the Causes and Impact of Network Failures. In *Proc. ACM SIGCOMM*.